DOD Privacy Impact Assessment (PIA)

1. Name of MACOM / DA Staff Proponent (APMS Sub Organization Name)

U.S. Army, Office of the Assistant G-1 for Civilian Personnel

2. Name of Information Technology (IT) System.

Civilian Productivity Report (CIVPRO)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

2800

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0690-200 DAPE, Department of the Army Civilian Personnel Systems

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 3013, Secretary of the Army
Army Regulation 690-200, General Personnel Provisions
Executive Order 9397

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of the system and components, and system backup)

The Civilian Personnel Productivity System (CIVPRO) provides monthly statistics on personnel workload at each Army Region. The CIVPRO data are compiled monthly from appropriated fund records in the Defense Civilian Personnel Data System (DCPDS) and

the HQ Army Civilian Personnel System (HQ ACPERS). The reports include Army-wide, Region Civilian Personnel Operation Center (CPOC), Civilian Personnel Advisory Center (CPAC), Command, and Unit breakouts. CIVPRO is an existing system that is in the operation and maintenance phase. The system contains information pertaining to Army civilian workforce personnel.

CIVPRO interfaces with DCPDS (DoD civilian workforce database repository) and HQ ACPERS (Army Civilian database repository) via a secure network connection. Users can access the system via a website. Web servers, application servers and database servers are located in Alexandria, Virginia.

Server event logs are checked daily by the system administrator / information assurance security officer (IASO). Back up tapes are run daily. Tapes are stored at a commercial site in Atlanta, Georgia.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.)

Information in identifiable form that will be collected includes: individual's name, gender, date of birth, national identifier, social security number (SSN), employee number, email address, telephone number, educational level, salary, discharge status, race/ethnicity, origin, position grade, position title and information relating to personnel actions regarding the individual. Information used by the system is extracted from the Headquarters Army Civilian Personnel Data System (HQ ACPERS) and the Defense Civilian Personnel Data System (DCPDS) via a secure network.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Information used by CIVPRO is extracted from DCPDS (DoD civilian workforce database repository) and HQ ACPERS (Army civilian workforce database repository) via a secure network. No information is collected directly from an individual.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).

This system allows the Army to properly gauge workload and accomplishment of work by civilian employees. The Office of the Assistant G-1 for Civilian Personnel was established under the Secretary of the Army to carry out these mandates. Information in identifiable form is collected and used by this system in direct support of these missions.

13. Describe how the information in identifiable form will be used (e.g. to verify exiting data, etc.).

Information in identifiable form will be used to produce a series of reports that aid Army leadership in identifying workflow problems and improving organizational performance. Reports are also used to monitor CPOC and Civilian Personnel Advisory Center (CPAC) productivity in the area of recruitment and filling jobs.

14. Describe whether the system derives or creates new data about individuals through aggregation.

The system does not derive or create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Information will be available to authorized users with a need to know in order to perform official government duties. Information is shared with Commanders of civilian employees. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Criminal Investigative Service, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable for about themselves or to contest to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Information in identifiable form is not collected directly from the individual thus individuals are not given the opportunity to object to the collection of information in identifiable form about themselves or to contest the specific uses of the information in identifiable form.

17. Describe any information that is provided to and individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of the delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

Information used by CIVPRO is extracted from DCPDS and HQ ACPERS. Individuals are not involved in this process. Individuals are provided privacy advisories upon initial employment, and at that time implicitly consent to the capture and use of this information.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This system has a current certification and accreditation. The system resides on a secure military installation within secure facilities. These facilities have armed guards that verify the credentials (appropriate DoD building/identification badge) of all employees and login all visitors including, vendors and maintenance. Users of this system include Army civilian personnelists and administrative technical support. Users are required to undergo and receive at a minimum ADP/IT III background investigation. These users (both government and contractor) may have access requirements and are limited to specific or general information in the computing environment. The system administrator defines specific access requirements dependent upon each user's role. Each specific application in the system may further restrict access via application-unique permission controls. Management users as well as system and database administrators must enter appropriate user/Identification and password before being authorized access to the resources. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, etc.). Additionally, all aspects of privacy, security, configuration, operations, data retention and disposal are documented to ensure privacy and security are consistently enforced and maintained. There is routine monitoring of security events, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIGs). Files transferred across the internet/NIPRNET are encrypted.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program" November 11, 2004. If so, and a System of Records Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when the publication of the notice will occur.

The system requires a SORN and it is published.

20. Describe/evaluate any potential privacy risk regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate and privacy risks in providing individuals and opportunity to object/contest or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data thus we believe the risk to the individual's privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risks are further mitigated by the implementation of firewalls, intrusion detection systems and malicious code protection.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.